

CLAIMS

What is claimed is:

- 1 1. A method of preventing an attack on a network, wherein the attack comprises sending
2 a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method
3 comprising the computer-implemented steps of:
 - 4 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
5 header is set;
 - 6 determining whether a sequence value in the packet is within a range of allowed
7 sequence values; and
 - 8 when the sequence value is within the range of allowed sequence values, sending an
9 acknowledgment message without closing a TCP connection associated with
10 the flow.
- 1 2. A method as recited in Claim 1, further comprising the steps of:
 - 2 receiving, from the remote end node, a next packet of a flow in which the RST bit is
3 set and comprising a second sequence value;
 - 4 determining whether the second sequence value is equal to an expected sequence
5 value; and
 - 6 closing a TCP connection associated with the flow only when the second sequence
7 value is equal to the expected sequence value.
- 1 3. A method as recited in Claim 1, wherein the range of allowed sequence values does
2 not include the expected sequence value.
- 1 4. A method of preventing an attack on a network, wherein the attack comprises sending
2 a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method
3 comprising the computer-implemented steps of:
 - 4 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
5 header is set; and

6 sending an acknowledgment message without closing a TCP connection associated
7 with the flow and without regard to whether a sequence value in the packet is
8 within a range of allowed sequence values.

1 5. A method as recited in Claim 4, further comprising the steps of:
2 setting a flag representing receipt of the packet with RST bit set;
3 receiving, from the remote end node, a next packet of a flow in which the RST bit is
4 set and comprising a sequence value;
5 determining whether the sequence value equals an expected sequence value; and
6 closing the TCP connection only when the sequence value equals the expected
7 sequence value.

1 6. A method as recited in Claim 5, further comprising the step of dropping the packet
2 and the next packet when the RST bit is set and the sequence value of the next packet does
3 not equal an expected sequence value.

1 7. A method as recited in Claim 4 or Claim 5, further comprising the steps of determining
2 that the RST bit is not set in the packet or the RST bit is set and holds an incorrect
3 sequence number, and in response thereto, clearing the flag.

1 8. A method as recited in Claim 1, further comprising the steps of accumulating a
2 counter that counts spurious TCP RST packets.

1 9. A method as recited in Claim 1 or Claim 8, further comprising the steps of generating
2 a notification message when the packet is not successfully validated.

1 10. A method as recited in any of Claims 1, 2, 3, 4, 5, 6, or 8, further comprising the steps
2 of generating a notification message when either the sequence value or the second sequence
3 value is not within the allowed range of sequence values.

1 11. A method of preventing an attack on a network, the method comprising the computer-
2 implemented steps of:

3 receiving, from a remote end node, a packet of a flow in which a SYN bit of a header
4 is set;
5 sending an acknowledgment message without closing a TCP connection associated
6 with the flow and without regard to whether a sequence value in the packet is
7 within a range of allowed sequence values;
8 receiving a next packet of the flow; and
9 when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim
10 4 with respect to the next packet.

1 12. A method as recited in Claim 11, further comprising the steps of taking no action with
2 respect to the TCP connection when the next packet is not a TCP RST packet.

1 13. A method as recited in Claim 11, further comprising the steps of accumulating a
2 counter that counts spurious TCP SYN packets.

1 14. A method as recited in any of Claims 11, 12, or 13, further comprising the steps of
2 generating a notification message when the packet is not successfully validated.

1 15. A method as recited in any of Claims 1, 4, or 11, wherein the steps are performed by
2 a router or switch in a packet-switched network.

1 16. A method of preventing an attack on a network, wherein the attack comprises sending
2 a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set, the method
3 comprising the computer-implemented steps of:

4 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
5 header is set; and
6 determining whether a sequence value in the packet is within a range of allowed
7 sequence values including the expected sequence value; and

8 when the sequence value is within the range of allowed sequence values including the
9 expected value, sending an acknowledgment message without closing a TCP
10 connection associated with the flow.

1 17. A method as recited in Claim 18, further comprising the steps of:
2 setting a flag representing receipt of the packet with RST bit set;
3 receiving, from the remote end node, a next packet of a flow in which the RST bit is
4 set and comprising a sequence value;
5 determining whether the sequence value equals an expected sequence value; and
6 closing the TCP connection only when the sequence value equals the expected
7 sequence value.

1 18. A method as recited in Claim 17, further comprising the step of dropping the packet
2 and the next packet when the RST bit is set and the sequence value of the next packet does
3 not equal an expected sequence value.

1 19. A method as recited in Claim 16 or Claim 17, further comprising the steps of
2 determining that the RST bit is not set or the RST bit is set and hold the incorrect sequence
3 number in the next packet, and in response thereto, clearing the flag.

1 20. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set,
3 comprising:
4 means for receiving, from a remote end node, a packet of a flow in which a RST bit
5 of a TCP header is set;
6 means for determining whether a sequence value in the packet is within a range of
7 allowed sequence values; and
8 means for sending, when the sequence value is within the range of allowed sequence
9 values, an acknowledgment message without closing a TCP connection
10 associated with the flow.

11

1 21. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit
3 set, comprising:
4 a processor;
5 one or more stored sequences of instructions that are accessible to the processor and
6 which, when executed by the processor, cause the processor to carry out the
7 steps of:
8 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
9 header is set;
10 determining whether a sequence value in the packet is within a range of
11 allowed sequence values; and
12 when the sequence value is within the range of allowed sequence values, sending an
13 acknowledgment message without closing a TCP connection associated with
14 the flow.

1 22. A computer-readable medium carrying one or more sequences of instructions for
2 preventing an attack on a network, wherein the attack comprises sending a spurious
3 transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution
4 of the one or more sequences of instructions by one or more processors causes the one or
5 more processors to perform the steps of:
6 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
7 header is set;
8 determining whether a sequence value in the packet is within a range of allowed
9 sequence values; and
10 when the sequence value is within the range of allowed sequence values, sending an
11 acknowledgment message without closing a TCP connection associated with
12 the flow.

1 23. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set,
3 comprising:
4 means for receiving, from a remote end node, a packet of a flow in which a RST bit
5 of a TCP header is set; and
6 means for sending an acknowledgment message without closing a TCP connection
7 associated with the flow and without regard to whether a sequence value in
8 the packet is within a range of allowed sequence values.
9

1 24. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit
3 set, comprising:
4 a processor;
5 one or more stored sequences of instructions that are accessible to the processor and
6 which, when executed by the processor, cause the processor to carry out the
7 steps of:
8 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
9 header is set; and
10 sending an acknowledgment message without closing a TCP connection associated
11 with the flow and without regard to whether a sequence value in the packet is
12 within a range of allowed sequence values

1 25. A computer-readable medium carrying one or more sequences of instructions for
2 preventing an attack on a network, wherein the attack comprises sending a spurious
3 transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution
4 of the one or more sequences of instructions by one or more processors causes the one or
5 more processors to perform the steps of:
6 receiving, from a remote end node, a packet of a flow in which a RST bit of a TCP
7 header is set; and

8 sending an acknowledgment message without closing a TCP connection associated
9 with the flow and without regard to whether a sequence value in the packet is
10 within a range of allowed sequence values.

1 26. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit set,
3 comprising:

4 means for receiving, from a remote end node, a packet of a flow in which a SYN bit
5 of a header is set;
6 means for sending an acknowledgment message without closing a TCP connection
7 associated with the flow and without regard to whether a sequence value in
8 the packet is within a range of allowed sequence values;
9 means for receiving a next packet of the flow; and
10 means for performing the functions provided by the means of Claim 20 or Claim 23
11 when the next packet is a TCP RST packet.

12

1 27. An apparatus for preventing an attack on a network, wherein the attack comprises
2 sending a spurious transmission control protocol (TCP) packet with a Reset (RST) bit
3 set, comprising:
4 a processor;
5 one or more stored sequences of instructions that are accessible to the processor and
6 which, when executed by the processor, cause the processor to carry out the
7 steps of:
8 receiving, from a remote end node, a packet of a flow in which a SYN bit of a header
9 is set;
10 sending an acknowledgment message without closing a TCP connection associated
11 with the flow and without regard to whether a sequence value in the packet is
12 within a range of allowed sequence values;
13 receiving a next packet of the flow; and
14 when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim
15 4 with respect to the next packet.

1 28. A computer-readable medium carrying one or more sequences of instructions for
2 preventing an attack on a network, wherein the attack comprises sending a spurious
3 transmission control protocol (TCP) packet with a Reset (RST) bit set, wherein the execution
4 of the one or more sequences of instructions by one or more processors causes the one or
5 more processors to perform the steps of:

6 receiving, from a remote end node, a packet of a flow in which a SYN bit of a header
7 is set;
8 sending an acknowledgment message without closing a TCP connection associated
9 with the flow and without regard to whether a sequence value in the packet is
10 within a range of allowed sequence values;
11 receiving a next packet of the flow; and
12 when the next packet is a TCP RST packet, performing the steps of Claim 1 or Claim
13 4 with respect to the next packet.

14